Vulnerability Assessment Report

Nessus (IP: 192.168.1.54)

Introduction

Purpose

Nessus is a widely used vulnerability assessment tool that scans computer systems, networks, and applications to identify security vulnerabilities and configuration issues. Its main purposes include vulnerability scanning, compliance checking, configuration auditing, malware detection, and sensitive data discovery. Nessus is developed by Tenable and is available in free and commercial versions with different capabilities.

Scope

- **Target System:** Windows 8
- **IP Address:** 192.168.1.54
- **Assessment Tools Used:** Nessus
- **Assessment Date:** 30th March 2025

Reconnaissance & Scanning

First you open our kali after we have downloaded the **"Nessus iso image".** Next, we write the

"ls" command to check the list of options.

We click on download to display our Nessus download.

```
┌──(kali㉿kali)-[~/Downloads]
└─$ sudo dpkg -i Nessus-10.8.3-ubuntu1604_amd64.deb
[sudo] password for kali:
(Reading database ... 419598 files and directories currently installed.)
Preparing to unpack Nessus-10.8.3-ubuntu1604_amd64.deb ...
Unpacking nessus (10.8.3) over (10.8.3) ...
Setting up nessus (10.8.3) ...
HMAC : (Module_Integrity) : Pass
SHA1 : (KAT_Digest) : Pass
SHA2 : (KAT_Digest) : Pass
SHA3 : (KAT_Digest) : Pass
TDES : (KAT_Cipher) : Pass
AES_GCM : (KAT_Cipher) : Pass
AES_ECB_Decrypt : (KAT_Cipher) : Pass
RSA : (KAT_Signature) : RNG : (Continuous_RNG_Test) : Pass
Pass
ECDSA : (PCT_Signature) : Pass
ECDSA : (PCT_Signature) : Pass
DSA : (PCT_Signature) : Pass
TLS13_KDF_EXTRACT : (KAT_KDF) : Pass
TLS13_KDF_EXPAND : (KAT_KDF) : Pass
TLS12_PRF : (KAT_KDF) : Pass
PBKDF2 : (KAT_KDF) : Pass
SSHKDF : (KAT_KDF) : Pass
KBKDF : (KAT_KDF) : Pass
HKDF : (KAT_KDF) : Pass
SSKDF : (KAT_KDF) : Pass
X963KDF : (KAT_KDF) : Pass
X942KDF : (KAT_KDF) : Pass
HASH : (DRBG) : Pass
CTR : (DRBG) : Pass
HMAC : (DRBG) : Pass
DH : (KAT_KA) : Pass
ECDH : (KAT_KA) : Pass
RSA_Encrypt : (KAT_AsymmetricCipher) : Pass
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass
INSTALL PASSED
Unpacking Nessus Scanner Core Components ...

 - You can start Nessus Scanner by typing /bin/systemctl start nessusd.service
 - Then go to https://kali:8834/ to configure your scanner
```

To run the Nessus download, we run a **“Sudō dpkg”** command, which is **“Sudō dpkg -I Nessus-10.8.3-ubuntu1604_amd64.deb."**

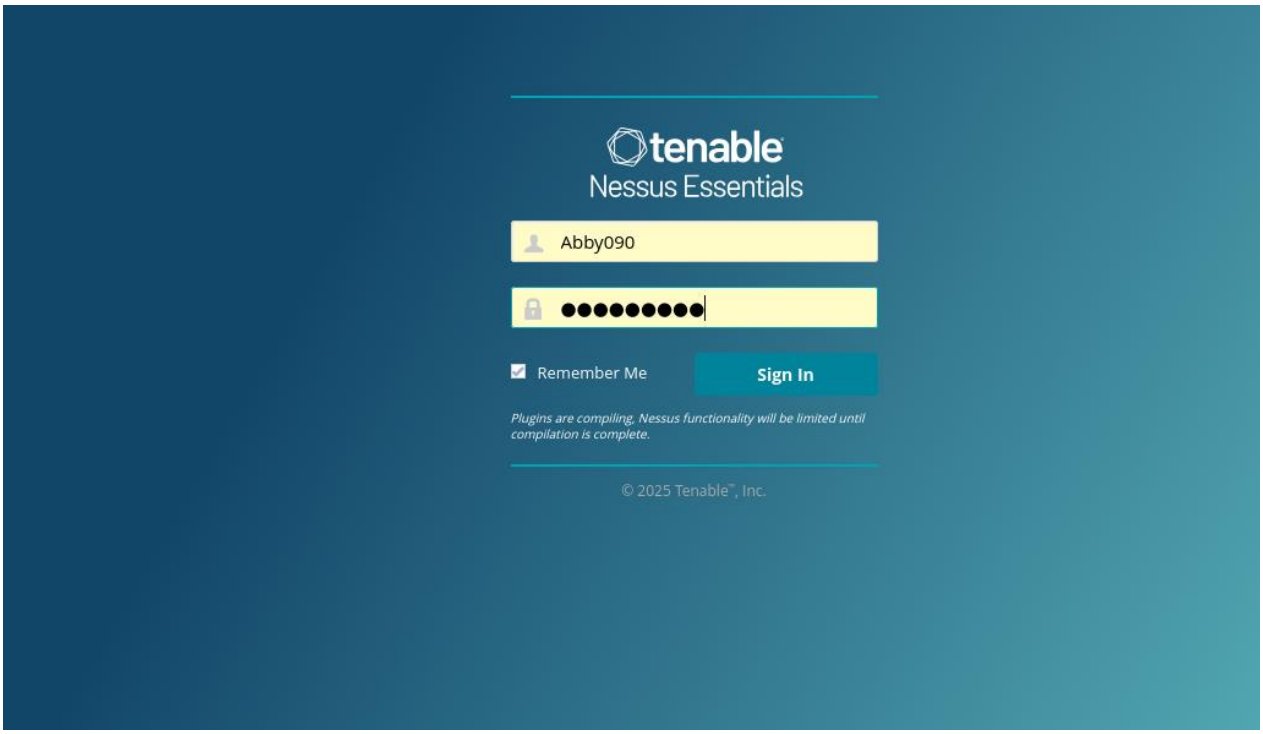
```
┌──(kali㉿kali)-[~/Downloads]
└─$ sudo systemctl start nessusd
```

After running the sudo dpkg command, it’s been passed. We will start the Nessus Scanner by typing **“sudo systemctl start nessusd."**

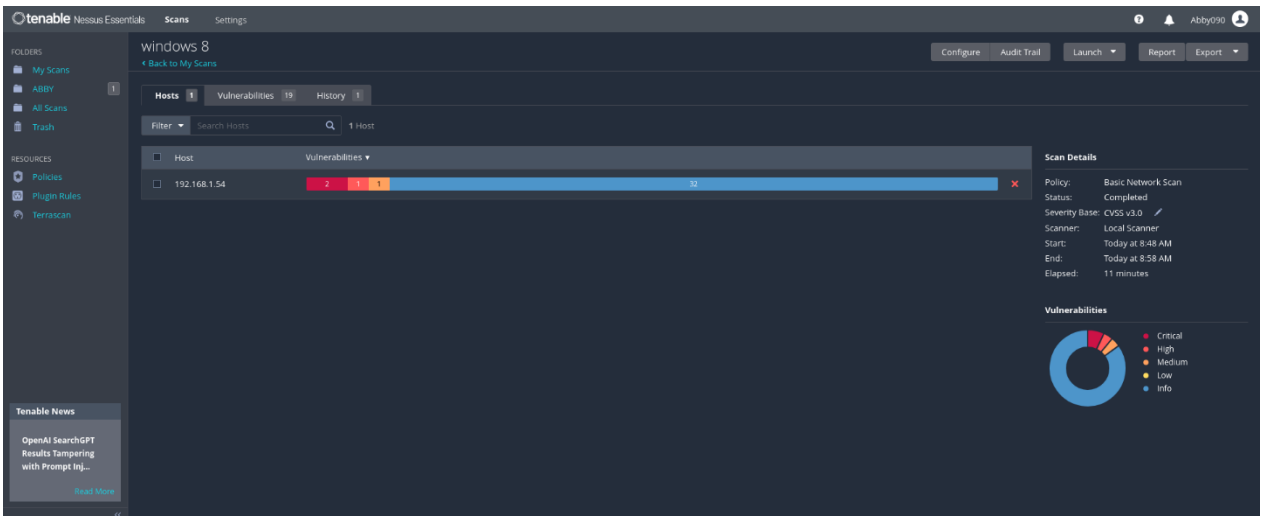
```
┌──(kali㉿kali)-[~/Downloads]
└─$ sudo systemctl status nessusd
● nessusd.service - The Nessus Vulnerability Scanner
     Loaded: loaded (/usr/lib/systemd/system/nessusd.service; disabled; preset: disabled)
     Active: active (running) since Mon 2025-03-17 19:28:38 EDT; 22s ago
 Invocation: b1ab4e225ec245a2a9e58ddae5ba9caa
   Main PID: 10780 (nessus-service)
      Tasks: 17 (limit: 2212)
     Memory: 672.5M (peak: 672.8M)
        CPU: 33.104s
     CGroup: /system.slice/nessusd.service
             ├─10780 /opt/nessus/sbin/nessus-service -q
             └─10783 nessusd -q

Mar 17 19:28:38 kali systemd[1]: Started nessusd.service - The Nessus Vulnerability Scanner.
```

This is to check the status of our Nessus to know if it's active and running. Running this, we run a **“sudo command,”** which is **“sudo systemctl status nessusd."**



After stating that the Nessus will bring out a login page to insert the login details to open the Nessus.



Here's a summary of the information in each row:

Start: The process is completed.

Security Base: The value is high.

Scanner: The scanner is local.

Start: The process started today at 848.00.

End: The process ended today at 858.00.

Planted: The process took 11 minutes.

Prepared by: Aliu A. Sanusi | Cybersecurity Analyst